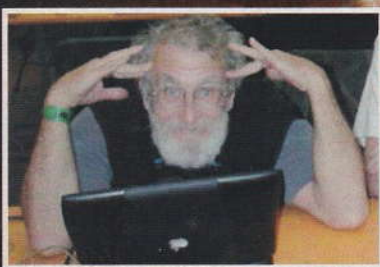
TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI
HACKER
JOUR
2 €
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI
PENETRATI I CHIOSCHI DELLE BIBLIOTECHE!
NIENTE È PIÙ SICURO: NEMMENO LE FIRME DIGITALI
PERSONAGGIO FAMOSO: CAP'N CRUNCH
COME FARSI UN BLOG 'SUPER'
SEGRETI DI GOOGLE: UN POZZO INFINITO
ALLA SCOPERTA DI FREEBSD
CINA
TRUCCHI E SEGRETI PER AGGIRARE LA CENSURA PIÙ RIGIDA DEL MONDO!
QUATTORDICINALE ANNO 3
16/29 DICEMBRE 2004 - SPED. IN ABB. POST. 70% - MILANO
IL PREZZO IN COPERTINA È VALIDO SOLO PER L'ITALIA
40065
9 771594 577001
4ever
HACKING DELL'ALBERO DI NATALE: EFFETTI DA SBALLO CON LUCI E PC

Anno 3 – N. 65
16/29 Dicembre 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale

Picchia tutto, **picchia duro**

Bristol, Regno Unito. Il giudice Roach non sente ragioni e condanna a sei mesi di carcere un ragazzo di diciannove anni. L'accusa? In aula di tribunale ha ripreso un'udienza con la videocamera integrata nel suo telefonino. Fesso lui, inflessibile il giudice.

Treviglio, Italia. Un piccolo imprenditore con l'unica colpa di avere un cognome identico a un famoso stilista cede di sua volontà alla pressione legale del più potente, dopo anni di costose battaglie giudiziarie, stanco di rovinarsi il fegato per un nome. Il proprio nome di dominio. Bella, la possibilità di avere un dominio con il proprio cognome. Peccato che se i potenti ne hanno uno uguale, il loro è più bello ancora.

Lycos, Pianeta Terra. Un salvaschermo scatena una battaglia senza esclusione di colpi ai siti da cui partono le email degli spammer. Bloccandone i messaggi? No, attaccando per primi. Piegandone la banda disponibile sotto il fuoco di gigabyte di traffico proveniente dai salvaschermo di tutto il mondo. Quelli di Lycos giurano che non è un attacco DDoS organizzato, ma sarebbe interessante capire qual è la percentuale di attacco sotto cui non si può più chiamare con tale nome. Nessuna simpatia per gli spammer, solidarietà all'iniziativa Lycos, seppure rimanga un certo scetticismo sulla vera utilità, ma anche questo è un segno dei tempi.

Tempi da far west, a leggerli bene. Perché qui non è più questione di difendere diritti e libertà dell'era digitale, ma di difendersi da chi di questa libertà ne fa macello.

Se non fosse Natale, diremmo che il mondo è sempre andato avanti così. Oggi, però, in digitale.

theguilty@hakerjournal.it

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea:
Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron Silvio De Pecher, Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo
Elenina "menosina" Varesi

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Distributore per l'estero:
Johnsons International News Italia Spa
Via Valparaiso, 4
20144 Milano - Italia

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Un futuro da GIOCARCI

Una tecnologia non risolverà i nostri problemi, ma quando ci si mettono di mezzo tre società come Sony, Ibm e Toshiba messe assieme c'è da credere che qualcosa di almeno originale ne debba venire fuori. Fosse solamente perché nel gruppo brilla l'assenza di sua maestà Microsoft, cosa che fa ben sperare nella reale freschezza e innovazione del progetto.
In realtà i soggetti in questione sono quattro, perché Sony è presente con le due facce di Sony Corporation e Sony Computer Entertainment, ma questi sono dettagli che dicono solamente quali investimenti di denaro sono stati messi sul piatto. Per fare cosa? La nuova Playstation 3, sostanzialmente.
Meglio, per ora si parla del nuovo processore che sarà il cuore della Playstation 3, ma anche di un mucchio di altri dispositivi, tra cui televisori mai visti prima e impianti multimediali da fare paura.
Il microprocessore in questione si chiama, in codice, Cell.
Tutte le specifiche verrano rivelate alla International Solid State Circuits Conference di San Francisco, che si svolgerà dal 6 al 10 febbraio dell'anno prossimo.
Per ora sono emersi solamente dei particolari, ma già fanno rumore.

Sostanzialmente le società hanno confermato che si tratta di un processore a 64 bit, in realtà formato da un cuore principale e diversi processori di contorno (le 'celle', appunto) tra di loro interdipendenti.
La capacità di calcolo pare sia impressionante, alcuni dicono paragonabile a quella di qualche attuale supercomputer, e quindi molto adatta ad applicazioni in cui si sprecheranno contenuti video e multimediali.
Per dirla con Ibm, l'attuale architettura dei pc sta per collassare sotto il peso delle richieste di multimedialità e banda larga che gli utenti si aspettano.
E dal laboratorio congiunto che Ibm, Toshiba e Sony hanno messo in piedi a partire dal 2001 ad Austin, in Texas, pare proprio sia giunto il momento dell'emersione di questo incredibile aggeggio tecnologico.
Per noi sarà già un divertimento scoprirne tutti i segreti.

Alcune specifiche tecniche di Cell

- architettura distribuita multiprocessore
- supporto di diversi sistemi operativi nello stesso momento
- trasferimento da e per la memoria alla massima velocità del bus
- I/O completamente flessibile
- sistema di controllo in tempo reale per applicazioni in tempo reale
- chip di protezione dei contenuti (anticopia?) integrato nel sistema

e molto altro ancora.

FreeBSD

Ciao a tutta la (fantastica) redazione di hackerjournal. Sono un assiduo lettore della vostra rivista. Ieri sfogliando fra i vecchi giornali ho notato quell'articolo sul condor che si era recato a Milano per la presentazione del suo libro (leggetelo perché è fantastico, ve lo assicuro). In una riga Kevin spiegava che lui usava Linux e FreeBSD. Sul computer ho sia WindozzoloXP (non mi sta simpatico, ma mi diverto a farci gli esperimenti), sia Linux. Così ho pensato : "perché non provare FreeBSD?". Mi sono connesso e ho cercato qualche informazione, solo che non ho trovato qualcosa di schematico. Ed ecco che arrivo al dunque: potete darmi qualche informazione a proposito? O, meglio ancora, invito i lettori che ne sanno qualcosa a mandarmi una e-mail al seguente indirizzo [reodark@virgilio.it]. Vi ringrazio tantissimo, siete mitici...
Reodark

Bene, capiti giusto giusto: guarda qualche pagina più avanti. Comunque stai certo che ci sarà anche qualche lettore interessato. I nuovi amici sono sempre graditi!

Qualche Suggerimento

Riceviamo moltissima posta, su tutte le caselle dedicate alla rivista. Per facilitarci il compito ed essere sicuri di venire letti, ricordiamoci che:

- **la posta va sempre firmata**; firma che siamo implicitamente autorizzati a riportare sulla rivista in caso di risposta pubblica;
- **a redazione@hackerjournal.it** inviamo tutte le richieste generiche, ma ricordiamoci che è anche la più trafficata;
- **a guestbook@hackerjournal.it** inviamo le soluzioni al cyberenigma, specificando bene nell'oggetto a quale numero si riferisce (esempio: "cyberenigma 65", non c'è bisogno di aggiungere altro);
- **i file e gli allegati è sempre meglio zipparli,** anche per evitare i filtri antivirus che ogni tanto eliminano file di provenienza poco chiara.
- **se vogliamo cimentarci a scrivere** articoli o mandare contributi, possiamo inviarli direttamente a one4bus@hackerjournal.it
- **la redazione è autorizzata** a tagliare e riassumere le lettere troppo lunghe per dare maggiore possibilità di pubblicazione;
- **evitiamo di inviare email** con la richiesta di conferma della lettura; ripetiamo che leggiamo tutti, ma se ciascuno ci chiede anche di confermare che lo abbiamo ricevuto, per leggervi tutti ci mettiamo il doppio del tempo...

Fatemi passare l'esame

Salve redazione, volevo chiedervi un aiutino per passare l'esame di programmazione dell'università... sto a ingegneria delle telecomunicazioni primo anno! è richiesto per aumentare il punteggio di fare un programmino in c per la gestione di videocassette... io vi spedisco il progetto se voi gentilmente tra un caffè e l'altro... tanto per voi sarà un gioco da ragazzi...
Paperino Topolino

Tra un caffè e l'altro il massimo che possiamo fare è lavorare... sorry, non siamo una software house e nemmeno ci chiamiamo Cepu.
Sotto con la volontà e non perdere altro tempo. Ingegneria richiede tutta l'attenzione e la concentrazione :)

Potreste...

Potreste compilarmi voi il sorgente e poi inviarmi l'eseguibile? Potreste anche modificarmi il sorgente in modo che a ogni avvio del mio computer si avvii il file per il controllo remoto...
Mangusta

Caro Mangusta e con te molti altri: ripetiamo che non possiamo dare seguito alle richieste di progetti, modifiche, programmazione, eccetera. Noi leggiamo tutta la posta (anche quella che inviate con la richiesta di ricevuta di ritorno: evitate, grazie). Solo che riceviamo centinaia di email al giorno e non possiamo rispondere sempre. Di tutto teniamo conto per fare meglio la rivista, comunque.

Spettroscopio due

Ciao! Con i vostri consigli ho creato uno spettroscopio e vi invio le foto! Pubblicatemi x favore!
Federico aka fox91

Delle foto che ci invii ne sono arrivate molte corrotte (vediamo solamente l'anteprima) e ne possiamo pubblicare una sola. Niente paura e complimenti, si vede che funziona proprio bene! Attendiamo le realizzazioni di altri lettori!

Clamwin antivirus

Salve redazione! Mi potete dire il sito dove posso aggiornare il mio antivirus clamwin per win perché quando ho aggiornato mi ha detto che la mia versione non è aggiornata. Aiutatemi grazie!
python_coah

Vai qui: www.clamwin.com

Hackers Magazine!

Salve. Volevo consigliare una bella cosa... Sono un vostro accanitissimo lettore, leggo HJ dal numero 3 (azz... i primi due numeri li ho persi, ma da allora lo prendo sempre... So che vendete moltissime copie di Hacker Journal in Italia... e volevo consigliare, una volta al mese, di allegare un cd-rom o un dvd-rom con all'interno molti molti software. (Non costerebbe tanto, dai...). Ho parlato con molti acquirenti di HJ e tutti questi vorrebbero il cd o dvd almeno una volta al mese! Che ne dite?
Antonio

Non ci piace fare pubblicità, ma data la richiesta non possiamo che segnalarvi l'esistenza di Hackers Magazine: è esattamente tutto quello che dite, e siamo sempre noi! ;)

Spettroscopio uno

Il mio spettroscopio funziona alla grande, complimenti per l'articolo! L'unica cosa che non capisco è che guardando qualsiasi fonte di luce lo spettro è sempre uguale: rosso verde blu (RGB), come mai?
Egidio

Ci mandi sei foto simili, ma non uguali! Per esempio, il Led rosso emette tra i 640 e i 700 nm (nanometri) e, infatti, nella foto che definisci 'strana' si vede una stretta zona tendente al rosso. Nelle altre, seppure simili (tutte lampadine al tungsteno?), se lo strumento fosse più preciso si vedrebbero delle bande più scure o più chiare di altre. Prova anche con lampade decisamente differenti, o prova a usare un tubo di cartone lungo, invece che una scatola di corn flakes. Sperimentare, è il nostro motto!

Adesso ci sono anch'io

Salve fighissima redazione di Hacker Journal. Sono un vostro nuovo lettore; la passione mi è nata comprando un numero di Hacker Journal Collection e da allora compro tutti i numeri.
Devo farvi notare un errore: nell'articolo Spia Mania apparso sul numero 44 lo "Spy Night Scope" costa 20$ mentre sul recente numero 62 all'articolo Spy Shopping lo "Spy Night Scope" costa 15$!!. Sono andato a vedere su Spygear e invece costa 14,95$!!. Spero che non facciate più questi errori (senza offesa).
Quasar
P.s Potreste indicarmi un sito da dove imparare il linguaggio Java? E magari anche un editor Java semplice semplice?
P.s.s Pubblicatemi vi prego!!

Salve a te Quasar, come potrai ben immaginare i siti e i prezzi sono due elementi che non vanno certo d'accordo con l'uniformità! Chissà quanti altri prezzi, in quanti altri siti, potremmo trovare differenti!
P.s. Qui trovi quasi tutto: www.mokabyte.it e un editor tra tanti anche qui www.studioware.com
P.s.s. Se poi era una scusa per farsi pubblicare... beh, eccoti accontentato. Grazie di averci scritto!

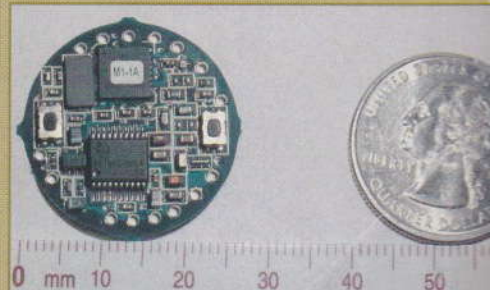
Password del Bios

Vorrei rispondere a Alakan (hj 63) che chiede se c'è una possibilità di rimuovere la pass al bios. Non so se ho capito bene di che pass si tratta, ma io so che per togliere la pass al bios basta togliere la batteria alla motherboard e tenerlo cosi un paio di minuti oppure accendere senza questa batteria, poi spegnere, rimettere la batteria e il gioco è fatto. (x HJ: Siete il no 1).
Lancelotu

Suggerimento sensato.

Grande Fratello rimandato?

Salve a tutta la redazione, ho appena letto l'articolo sulla nuova tecnologie degli impianti di riconoscimento sottocutanei e devo dirvi che c'è "un'imperfezione".
Le trasmittenti in questione, come avete detto voi, sono piccolissime e non hanno una batteria interna, generano i segnali necessari tramite il campo elettromagnetico del lettore nelle prossimità. Il punto è proprio la prossimità: secondo i ricercatori stessi, il campo di azione di questi apparecchi è di una decina di centimetri, pochi per poter veramente parlare di un sistema alla "grande fratello".
Ci tenevo solo a fare questa piccola precisazione, non c'è niente di sbagliato, ma, per la sua bassa scalabilità, al momento la situazione non è pericolosa come descritta.
Gengis Dave

Consigliamo la lettura, per esempio, di www.foodnavigator.com/news/news-NG.asp?n=50190-a-breakthrough-in. La lettura avviene a 11 metri di distanza. Sono risultati in condizioni particolari, ma risalgono a parecchi mesi fa. Con un lettore minuscolo come quello che riportiamo in foto, è possibile leggere già da 6 cm di distanza. Con un lettore come quello che troviamo all'indirizzo www.aurelia-micro.it/rfid/english/products_reader.php si raggiungono i cinque/sei metri. Di questo passo...

INDOSSIAMO UN DISPLAY

A Los Angeles non fanno altro che inventare le mode più intriganti. Nyx si prepara al 2005 con un giaccone che porta sulla schiena una display flessibile e programmabile, alimentato a batterie. Uno sballo, poter lanciare messaggi variabili secondo l'umore del giorno!

OCCHIALI VIDEO A TRE DIMENSIONI

Una parte è un display e una parte l'unità di controllo, delle dimensioni di un pacchetto di sigarette. Questa ha un'uscita video 640x480 e degli ingressi audio e RGB. I display, uno per occhio, hanno le dimensioni di un centimetro quadro, ma l'effetto che danno è quello di uno schermo da 42" visto alla distanza di due metri. Si è immersi, quindi. Lo scopo è quello di poter vedere qualunque immagine sia stata preparata per essere vista in 3D e con gli opportuni accorgimenti per essere divisa in due immagini "sfalsate". Con quattro batterie stilo, l'autonomia è di cinque ore di visione stereoscopica. Video Eyewear, così si chiama, è di provenienza giapponese, ma sarà disponibile a breve anche su un sito americano e venduto esclusivamente on-line all'indirizzo www.icuiti.com.

EXPLORER 6.0 "IL GRUVIERA"

Ricco di buchi. Come spesso accade, le versioni più recenti dei prodotti Microsoft sono vulnerabili. Così Microsoft Internet Explorer 6.0, quando "Salva immagine con nome" toglie l'ultima estensione e nel caso ne esista più d'una, usa quella contenuta nell'Url da cui stiamo scaricando l'immagine. Se, come la maggior parte degli utenti, abbiamo disabilitato la visibilità delle estensioni dei file (scelta peraltro di default), non possiamo accorgerci che l'estensione del file scaricato può tranquillamente essere un .exe, o peggio ancora. Immettendo così a nostra insaputa un bel programma pronto a partire sul nostro computer non appena pensiamo di aprire la finta immagine.
Le autorità finlandesi sono arrivate addirittura a invitare il settore pubblico a non utilizzare più quella versione di prodotto Microsoft. Passiamo in fretta a OpenSource, facciamo prima.

CELLULARI LINUX

DoCoMo, NEC e Panasonic sono alleati in Giappone per sviluppare un numero sempre maggiore di modelli di cellulari basati su Linux. La flessibilità della piattaforma Linux consente di dare ai nuovi telefonini delle funzionalità che hanno dell'incredibile:dall'audio 3D alla connessione integrata WiFi, al VoiP che consente telefonate via Internet fino a che si sta in una zona coperta dal wireless. Quando la copertura viene meno e la linea cade, una funzione automatica richiama l'utente sul numero di rete mobile tradizionale.

HOT NEWS

APRIAMO L'AUTOMOBILE A PUGNI

Abbiamo lasciato le chiavi dentro la macchina? Le abbiamo perse? Niente paura: qualche colpetto ben assestato sul vetro o sulla carrozzeria e le serrature scatteranno come d'incanto. Knock-In-Key costa quasi cento dollari, ma ci eviterà un sacco di seccature e perdite di tempo. Si tratta di un'idea tanto semplice quanto geniale: un sensore viene attivato da una sequenza programmabile di colpetti sul vetro, dati con le nocche delle dita. Se la sequenza è corretta, scatta il comando d'apertura. Lo troviamo su www.knockinkey.com.au
Altroché codici cifrati!

BASTA VHS

Abbiamo in casa enormi collezioni di videocassette con i filmini originali creati in anni e anni di riprese?

Malissimo: ci conviene correre ad acquistare qualunque cosa sia disponibile per trasformarle in DVD, perché ormai la cassetta è in precipitoso declino. Uno dei maggiori distributori di prodotti Hi-Fi in Inghilterra, Dixons, ha addirittura deciso di non vendere più videoregistratori VHS. Solamente DVD, già da questo Natale.
Segno dei tempi.

FIREFOX SPIONE IN GERMANIA

La versione tedesca di Firefox è stata accusata di contenere uno spyware. Effettivamente un accordo di Mozilla con eBay prevede di aggiungere al browser un pulsante per la navigazione immediata sul sito di eBay, a fronte anche di un invio a un database di report statistici anonimi sull'utilizzo del sistema. La comunità degli utenti tedeschi è naturalmente insorta contro questo innocuo, ma antipatico modo di gestire una pratica commercialmente interessante, ma effettuata all'insaputa degli utenti. Sono bastati pochi giorni perché Mozilla corresse ai ripari, scusandosi con gli utenti e attivando un meccanismo tale per cui l'invio dei dati avverrà solamente dopo richiesta di consenso all'utente.

UNIVERSITÀ DELL'HACKING

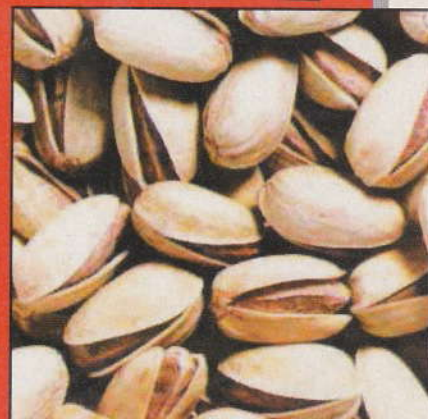
Finalmente qualcuno che distingue i pirati informatici dagli hacker. Così Ralph Echemendia dell'International Council of E-Commerce Consultants, www.eccouncil.org, ha organizzato dei corsi di hacking e prevenzione degli attacchi informatici. In cinque giorni si studiano le tecniche d'intrusione, la creazione di una policy di sicurezza, gli attacchi DDoS, i buffer overflow, la creazione dei virus, l'ingegneria sociale e così via. Peccato che il corso costi qualcosa come 4 mila dollari e sia quindi, di fatto, indirizzato a esperti di sicurezza o presunti tali di grandi società. Un altro sistema per fare soldi o una iniziativa costosa, ma lodevole?

Attendiamo qualche iniziativa analoga anche per i comuni mortali, hacker o aspiranti tali. Comunque alla fine si ottiene un diploma di Hacker Etico e ci sfugge la necessità dell'aggettivo. Non dicono di distinguere già in partenza tra hacker e pirati? Mah.

IPOD È PER L'ORECCHIO

Ciò che abbiamo visto in Matrix è robetta da nulla. "Scopo" è il nome di un monitor indossabile che promette di metterci a disposizione il video come iPod ci mette a disposizione l'audio.
Nei filmati di presentazione lo si vede addosso a un'improbabile casalinga con tanto di borsa della spesa, che naviga sulle liste degli acquisti e consulta le pagine gialle, passeggiando tranquillamente per strada.
Si collega a qualunque dispositivo abbia la possibilità di pilotare un monitor, tanto che Mitsubishi lo paragona all'iPod dell'occhio: sicuramente vorrebbe sognare un'analoga diffusione.

RISOLTO IL PISTACCHIO!

Tutti noi abbiamo maledetto i pistacchi chiusi. Perché quando sono chiusi sono proprio chiusi e spesso è difficile aprirli persino con lo schiaccianoci. Finalmente qualcuno ci ha pensato. Tom Pearson, un ingegnere impiegato allo US Agricultural Research Service di Manhattan, nel Kansas, ha costruito un aggeggio che fa cascare ogni pistacchio, al ritmo di 25 al secondo, su una piazzola metallica. Un microfono rileva il suono prodotto e un sofisticato software riconosce quello di un pistacchio chiuso da quello di un pistacchio aperto, attivando un semplice sistema di raccolta differenziata.

FALLE A RAFFICA

negli ALGORITMI CRITTOGRAFICI

MD5 è una specie di "sintesi" di qualunque documento gli si faccia digerire. Nel senso che tramite un calcolo matematico prende un messaggio di lunghezza arbitraria e produce come risultato una specie di impronta digitale del documento lunga 128 bit e, l'abbiamo creduto fino ad oggi, unica. Una descrizione completa la possiamo trovare all'indirizzo www.faqs.org/rfcs/rfc1321. Quattro ricercatori cinesi hanno però scritto un documento in cui si dimostra come, letteralmente, prendere in giro l'algoritmo. Così da due documenti differenti in realtà sarebbe possibile ottenere due firme uguali: il che ovviamente farebbe di colpo cadere ogni possibilità di usare MD5 per scopi minimamente seri.
Cosa potrebbe accadere di fronte a un giudice, se potessimo dimostrare che qualcuno poteva falsificare la firma spacciando un documento per nostro? O cosa potrebbe accadere se scaricassimo un file da Internet credendo di usufruire delle garanzie della stringa MD5, e invece in realtà scaricassimo un bel trojan distruttivo confezionato apposta per avere la stessa firma del file che stavamo cercando? Se il documento dei cinesi è da ritenersi valido, migliaia e forse milioni di file MD5 e dei loro file di origine andrebbero rimossi dal web, ricontrollati e sostituiti da qualcosa di più sicuro. Un gran casino.

E c'è di più. Quest'anno è stato dimostrato, da parte di Eli Biham e Rafi Chen, ricercatori israeliani, che l'ancor più famoso algoritmo SHA-1, rietnuto sicuro, ha dei punti di vulnerabilità finora ignoti. Questo implicherebbe, per esempio, che nemmeno i popolari programmi PGP e SSL possono più considerarsi sicuri. SHA-1 è stato perfino certificato come algoritmo sicuro dall'istituto nazionale degli standard americano, producendo una stringa in uscita dal documento lunga ben 160 bit. Eppure è attaccabile.

MD5 e SHA-1 sono algoritmi finora riconosciuti praticamente a prova di bomba, perché un solo cambiamento nel

Il popolare MD5 utilizzato nelle firme digitali non è così sicuro come dovrebbe. Fin dall'inizio qualcuno potrebbe aver saputo che si basa su algoritmi matematici insicuri

comunità internazionale.
Se approfondendo le vulnerabilità di SHA-1 si scoprissero dei buchi analoghi a quelli che hanno fatto abbandonare la precedente versione SHA-0, basterebbe una piccola rete di attuali pc per scardinare in tempi ragionevoli qualunque applicazione basata sull'algoritmo in questione.

I problemi di MD5 potrebbero coinvolgere un sacco di server, per esempio tutti quelli che montano Apache Web server, il quale fa uso degli algoritmi di MD5 per garantire gli utilizzatori che i codici sorgente di dozzine di siti mirror contengono file identici agli originali e sono quindi sicuri da utilizzare.
Sistemi come il "Solaris Fingerprint Database", lo strumento che garantisce la sicurezza dei file dell'ambiente operativo Solaris, interamente basati su MD5, potrebbero di colpo trovarsi nell'imbarazzante situazione di dover spiegare agli utenti come fare a garantire l'unicità dei propri file a fronte dell'uso di un algoritmo che crea cloni con una notevole facilità. Per l'algoritmo MD5, a sentire i ricercatori, poche ore su un pc standard sono sufficienti a garantire un'elaborazione sufficiente a creare cloni di qualunque firma digitale. Che in generale fossimo in una situazione insicura, lo si poteva anche supporre.
Che lo fossimo a questo livello, è veramente preoccupante.
Anche perché i documenti riguardanti la vulnerabilità sono di dominio pubblico e poco ci vorrà che qualche organizzazione ne approfitti per sferrare massicci attacchi. Da mettere ormai in conto.

messaggio originale dovrebbe produrre una impronta digitale completamente diversa, sia che si parta da una email o da un file di sistema operativo.
Invece no. Ora non è più possibile dire con sicurezza che questi sono algoritmi utili alla sicurezza. In sostanza è come se ormai potessimo clonare le firme digitali, con una operazione che produce le cosiddette collisioni.
Tutti hanno sempre saputo, naturalmente, che nessun algoritmo può essere dichiarato completamente sicuro. Ma si è sempre pensato che questo difetto potesse innanzitutto derivare dal tempo necessario a creare un risultato sballato, ovvero una collisione. Se una cosa si può fare, ma ci si impiega un tempo molto lungo, talmente lungo che il risultato non è più utilizzabile da chi ha iniziato il lavoro di scardinamento, è evidente che difficilmente serve a qualcosa. Quindi l'algoritmo è da considerarsi sicuro.

Il sistema SHA-1 richiede al computer che lo calcola di far girare le routine di cui è costituito almeno 80 volte, fino a creare la firma univoca. Biham, il ricercatore israeliano, è stato capace di duplicare una firma digitale in soli 30 degli 80 passaggi previsti. Lasciando di stucco la

Web Block

La Cina attua una rigida censura su Internet e i suoi contenuti. Ecco dove e come. Ci sarà anche un perché ?!?

Se pensiamo che il nostro sito possa venire visto in tutto il mondo e quindi anche dai cittadini cinesi, beh, non è detto. La Cina attua una violenta politica di censura nei confronti dei contenuti che arrivano dal mondo libero e può darsi che le nostre pagine siano bloccate.

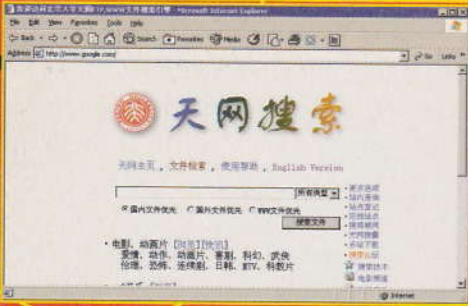
Modalità del blocco

Normalmente, se la homepage di un sito è bloccata, sono bloccate anche le pagine interne che stanno su quell'host. Non è vero il contrario, però. Questo filtro viene applicato sugli indirizzi IP dell'host più che sulla base dei nomi di dominio. Quando un singolo server ospita più siti, infatti (si pensi alle società di hosting), basta che un singolo sito sia filtrato perché lo siano anche tutti gli altri.
Esiste inoltre una modalità ulteriore di filtro, che analizza il contenuto delle pagine. Lo prova il fatto che esistono siti perfettamente visibili, con l'eccezione di alcune pagine precise.

Falle occasionali

Succede che un sito possa essere disponibile tramite un proxy e bloccato tramite un altro proxy. Non è chiaro se questo risponde a logiche regionali (si bloc-

MTU PIU BASSA E TUTTO PASSA... SPERIAMO

Alla pagina **http://www.cisco.com/warp/public/105/38.shtml** si trova una spiegazione approfondita di come abbassare l'MTU dello stack TCP/IP in modo che ogni pacchetto contenga meno dati del solito e sia quindi più difficile analizzare il traffico alla ricerca di parole proibite. Il costo di questa tecnica è però un aggravio del traffico e un rallentamento delle prestazioni.

ca il materiale ritenuto disturbante solo per una certa area) o se riflette una difficoltà di propagare per tutta la rete cinese la lista nera dei siti da bloccare. In vari hotel frequentati principalmente da occidentali, tra l'altro, le restrizioni sono molto minori.

Comunque sia, quando un sito viene bloccato, le autorità cinesi ne dirottano l'indirizzo, ossia i server DNS riportano per quelle pagine numeri DNS diversi da quelli realmente assegnati al sito. Quando un utente in Cina richiede un sito dirottato, al suo computer viene detto che al sito in questione è associato l'IP 64.33.88.161. Il numero corrisponde al sito http://www.falundafa.ca. Questo è un sito canadese che promuove la pratica religiosa del Falun Gong, setta che all'interno della Cina è vista con sfavore dalle autorità. Il sito è a sua volta bloccato e così la richiesta dell'utente non viene esaudita.

Come aggirare il blocco

Il blocco sulla base dell'indirizzo IP del server non è semplice da aggirare. Tendenzialmente, i pacchetti relativi a un IP proibito vengono ignorati. Il metodo tipico di aggiramento consiste nel canalizzare il traffico proibito su server proxy situati fuori dalla Cina. Tuttavia le autorità cercando di sorvegliare l'uso di questi proxy e la loro tenuta non è certa. Un metodo interessante era usare la cache di Google, ma da tempo i cinesi lo impediscono.

Sul filtraggio degli indirizzi IP dei server DNS la questione è più semplice. Per esempio si può provare a digitare l'indirizzo IP del sito anziché il suo nome, a patto che il sito non risieda su una macchina filtrata. Oppure ricorrere a server DNS non cinesi configurati per aggirare il problema.

Il filtraggio delle parole chiave dentro gli URL si può aggirare usando vie alternative per specificare i caratteri, per esempio scriverli in forma esadecimale (escaping). L'escaping serve anche agli autori dei siti; se codificano il testo in esadecimale o altro, possono sperare di sfuggire al filtraggio delle parole chiave in arrivo da un sito che non si vuole venga consultato. Più complicato e più ingegnoso, si può ridurre l'MTU dello stack TCP/IP, in modo che ogni pacchetto contenga meno testo e sia più difficile da ispezionare, a patto però di accettare una perdita nelle prestazioni e un sovraccarico di traffico di rete.

Speriamo che, come già è successo nel blocco orientale, alla lunga crolli anche la dittatura cinese; nel frattempo è dovere morale, per chi può farlo, impegnarsi perché anche in Estremo Oriente sia possibile avere una vera libertà di informazione e di Web.

NeOkOn
neOkOn@hacker journal.it

△ *Cercando le parole sbagliate con Google, in Cina bloccano i siti che le contengono.*

PRESTO, ESCAPPIAMO!

La RFC 2396, relativa alla specifica del protocollo HTTP (http://www.ietf.org/rfc/rfc2396.txt), specifica nella sezione 2.4.1 che i caratteri in un URL si possono inserire anche con codifiche diverse dal solito ASCII. per esempio, se un carattere ASCII ha codice esadecimale 4A, si può scrivere in un URL nella forma %4A. Può capitare che la censura cinese non colga la differenza e lasci passare l'informazione proibita.

GOOGLE STILE HACKER

Tutto quello che si può fare con il motore di ricerca più cliccato della rete

I lamer pensano che Google sia una casella dove scrivere testo da cercare. È molto di più!

Roba facile

http://www.google.it/preferences
Possiamo scegliere la lingua in cui parla Google, cercare solo pagine in una o più lingue, cambiare il numero di risultati mostrati in una ricerca ed eventualmente mostrare il risultato in una finestra diversa.

http://www.google.it/features
Google funziona anche come calcolatrice! Sa tradurre le pagine in un'altra lingua e sa cercare tipi di file specifici. Nella casella di ricerca digitiamo, insieme alle parole da cercare, filetype:pdf per cercare dentro file PDF, filetype:doc per cercare dentro file Word .doc e così via. Si dice che cercando dentro file .xls si possano trovare informazioni riservate su molte aziende…

Ancora, scrivendo link:www.hackerjournal.it possiamo vedere tutte le pagine linkate alla pagina principale del sito di HJ (non è possibile cercare testo, però). Invece, scrivendo site:www.gdrfantasy.it, cerchiamo all'interno del sito o del dominio in questione. Usando, infine, il pulsante Mi sento fortunato, Google visualizza solo le pagine che secondo lui corrispondono veramente a quello che volevamo trovare.

CHE COSA FA IL VERO HACKER CON GOOGLE

Il vero hacker scarica le API di Google dall'indirizzo http://www.google.com/apis/ e poi si scatena. Bastano infatti poche righe di Perl o di linguaggi ugualmente adatti peer sfruttare le capacità di Google in modo sconosciuto a qualunque comune mortale. In un prossimo articolo parleremo esattamente di questo e di come ottenere risultati spettacolari.

Roba più interessante

Invece di caricare http://www.google.it, usiamo http://www.google.com. Sopra la casella di ricerca, tra i link cliccabili, c'è l'opzione More… da cui si arriva a un sacco di possibilità in più. Anche se alcune funzionano solo per gli USA, vale la pena di esplorarle.

La calcolatrice non è solo una calcolatrice! Se scriviamo 5000 miles in kilometres, converte miglia in chilometri. 160 pounds * 400 feet in Calories calcola quante chilocalorie genera una forza di 160 libbre (circa 70 chili) applicata su una distanza di 400 piedi (circa 130 metri).

Possiamo cercare le pagine contenenti le definizioni di un termine scrivendo define e poi il termine da cercare. Possiamo ottenere invece una lista di definizioni scrivendo define: e, senza spazi in mezzo, il termine da cercare. La differenza è tra define hacker e define:hacker, e si vede tutta.

Google.com cerca inoltre indirizzi di persone, numeri di telefono americani, traccia spedizioni di corrieri come FedEx o UPS, trova targhe automobilistiche, prefissi telefonici, numeri di brevetto, numeri di registrazione dei velivoli e identificativi di apparecchi elettronici per la comunicazione! Il tutto solo per gli USA.

Funziona invece per tutto il mondo la ricerca di aeroporti: inserendo la sigla di un aeroporto seguita da airport, compaiono le pagine di riferimento per quell'aeroporto. Per esempio, mxp airport trova Malpensa. Se il volo è americano, lo si può tracciare, scrivendo, per esempio, delta 48 (compagnia e numero del volo).

Roba sempre più interessante

Google contiene risorse e possibilità non conosciute da tutti, che si trovano riassunte alla pagina http://www.google.com/options/index.html.

Gli Alert inviano una mail ogni volta che Google News ha un aggiornamento su una notizia di attualità. Google Answers mette un team di esperti a rispondere a pagamento alle nostre domande; nei Google Labs si trovano numerose tecnologie in via di sperimentazione, che potrebbero finire per diventare opzioni regolari di Google in futuro. Ci sono ricerche speciali dedicate a governo USA, Linux (google.com/linux), BSD (/bsd), Macintosh (/mac.html) e Microsoft (/microsoft.html); si possono effettuare ricerche nei documenti scientifici prodotti dalle università; una sezione ancora in beta permette di usare Google via cellulare.

Insomma, Google non è solo uno stupido motore di ricerca, ma un forziere pieno di tesori. E ne abbiamo appena scalfito la superficie.

P. Greco
p.greco@hackerjournal.it

Larry Page e Sergey Brin. Erano due studenti squattrinati, hanno creato un mondo nuovo per i naviganti in Internet.

IL TRUCCO DELLE DIECI PAROLE

Google riconosce solo le prime dieci parole digitate nel campo di ricerca e non va oltre. Ma possiamo usare l'asterisco (*) per indicare una parola qualunque, senza che conti nel limite. Supponiamo di dover cercare una canzone semisconosciuta digitandone i primi versi (nell'esempio useremo una canzone nota, per rendere chiaro il concetto). Digitiamo respiri piano senza far rumore ti addormenti di sera ti risvegli col sole… ma sono tredici parole e Google non le considera tutte. Se invece digitiamo respiri piano senza far rumore * addormenti * sera * risvegli * sole, per Google le parole sono solo nove, anche se in mezzo ci sono gli asterischi… e troveremo ugualmente il testo.

Il 3D delle FIRME

Tempi duri per i falsari; l'antica arte della miniatura non sarà più sufficiente per falsificare la firma su assegni, carte di credito e documenti. La riproduzione del profilo 3D di una firma sarà riservato a pochi e ricercatissimi esperti.

Le tecnologie più avanzate permetteranno di sconfiggere per sempre un'intera categoria di falsari: quelli delle FIRME ALTRUI

Nella perenne guerra tra le guardie e i ladri, la tecnologia sta per assestare un colpo bello duro ai falsari e in particolari agli imitatori di calligrafie, quelli che craccano assegni e carte di credito. Si vede già anche nei gialli televisivi più banali come i fogli sottostanti a quello su cui la vittima (o l'assassino) hanno scritto conservino traccia del messaggio, perché la scrittura non è solo bidimensionale sotto forma di traccia inchiostrata, ma a tre dimensioni. Chi scrive fa anche pressione sulla carta, e imprime una traccia di una certa profondità, minima ma misurabile. La notizia scontata è che questa profondità è personale e varia da scrivente a scrivente. Quella meno scontata è la possibilità di riconoscere la calligrafia e individuare le contraffazioni in base alla traccia tridimensionale del messaggio.

Signore e signori, la microprofilometria

La nuova tecnica è denominata microprofilometria 3D e ci stanno lavorando ricercatori dell'università italiana di Roma Tre. Secondo loro potrebbe assumere un ruolo decisivo nella lotta ai falsari. Il primo passo consiste nel realizzare un modello tridimensionale della pressione applicata durante la scrittura del testo.

La firma in tre dimensioni fornisce informazioni molto più chiare, rispetto alla sola traccia di inchiostro, rispetto alla sovrapposizione e direzione dei tratti di penna. Questi elementi vengono usati correntemente nel riconoscimento convenzionale della calligrafia, ma sovente sono confusi o non correttamente ricostruibili senza l'indicazione decisiva della terza dimensione.

Invece nel modello 3D sono ben visibili gli avvallamenti e le creste create durante la scrittura, così che diventa semplice ricostruire la formazione della firma, e lasciando intatto il campione di partenza, cosa che le tecniche finora usate non sempre garantiscono. In molte situazioni è impossibile avere a disposizione il possessore legittimo della firma (si pensi alle disposizioni testamentarie) e quindi conservare l'integrità del campione.

Addio ricalco

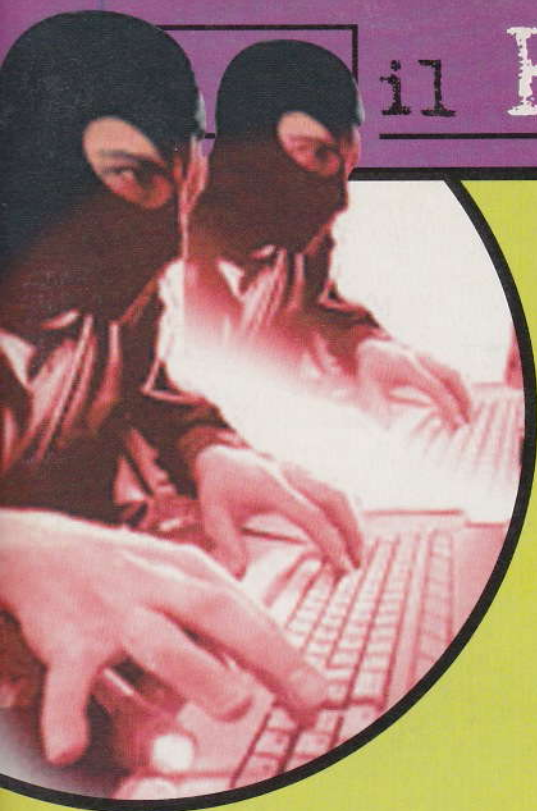
I falsari della scrittura da sempre imparano a ricalcare le firme, ma ultimamente hanno preso a utilizzare anche metodi evoluti di copia a mano libera. Però, aggiunta la terza dimensione, la loro missione diventa presto impossibile. Il falsario ha tipicamente poco tempo tempo e poche risorse. In queste condizioni, con cavolo che riescono a riprodurre un profilo 3D di una firma.

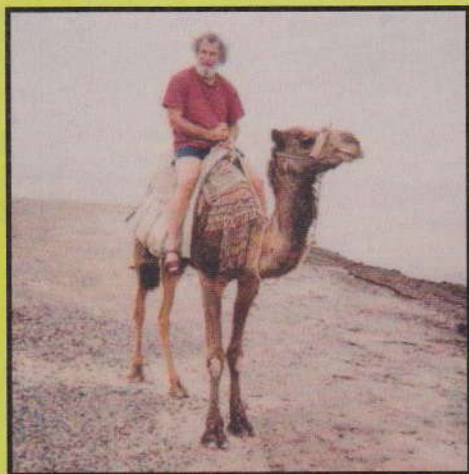
Al perito calligrafico della polizia, all'opposto, potrebbero bastare un paio d'ore di analisi per produrre un risultato incontestabile e privo di ambiguità.

L'apparecchiatura usata per ricavare le tracce 3D della scrittura a mano. Ingredienti principali, laser e modulo conoscopico.

Le prime applicazioni della microprofilometria 3D sembrano assai promettenti. La percentuale di riconoscimento corretto supera infatti già il 90 percento, su un corpus sperimentale di 126 lettere scritte da altrettanti autori differenti, che comprende certo le prevedibili penne a sfera ma anche stilografiche e persino pennarelli, su supporti che vanno dalla carta comune agli assegni fino al cartone pressato.

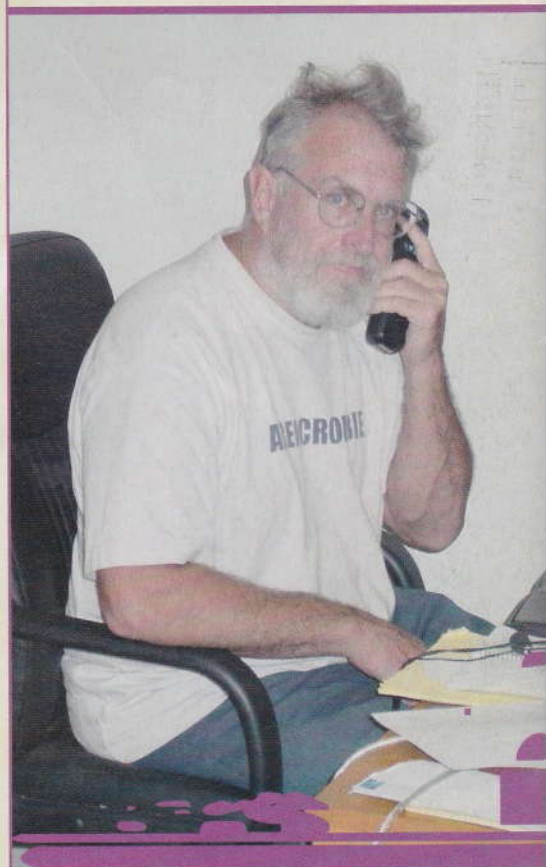
La scrittura con penna a sfera su carta comune è la combinazione più facile, dove il riconoscimento avviene con certezza praticamente assoluta. Insomma: in futuro il furto della carta di credito e altri problemi simili causerà meno danni, grazie alla firma tridimensionale che lasciamo senza saperlo quando scriviamo nelle due dimensioni del foglio di carta.

Reed Wright
reedwright@mail.inet.it

La carta igienica

In quei tempi, gli anni '70, i personal computer non esistevano e tanto meno Internet. Ma hacker si poteva essere lo stesso.

Gli hacker smanettavano sui sistemi universitari, tipo quelli telefonici di Ma Bell, la compagnia che aveva il monopolio sulle comunicazioni telefoniche all'epoca.
John era rimasto affascinato dalle possibilità di spostarsi all'interno della rete telefonica e aveva cominciato a sperimentare con i numeri per vedere cosa succedeva componendo, ad esempio, dei prefissi non previsti. Stava per scoprire un nuovo mondo, pieno di segreti.

John Draper ricevette da un certo Danny un numero telefonico strano, che lo collegava a una primordiale chat telefonica, dove c'erano persone che usavano parole mai sentite: loop, tandem, toni...
Incuriosito, John andò a casa di Danny: era un ragazzino, cieco, che stava lì nella sua camera con altri due amici a smanettare con il telefono e con una pianola. Suonando la pianola riuscivano a infinocchiare i dispositivi della centrale telefonica e telefonavano gratis in tutti gli Stati Uniti!
Inutile dire che si fece spiegare tutto e cioè che se si inviava un tono a 2600 Hz la centrale pensava che la linea fosse libera, quindi non conteggiava la chiamata.
Primo complice era stato un fischietto che si trovava dentro le scatole dei cereali Cap'n Crunch: per una di quelle combinazioni che il destino approva, emetteva il tono giusto.

La bluebox

Sapute queste e altre cosucce John, che era un hacker anche nell'elettronica, se ne andò a casa a spippolare con resistenze, transistor e regolo calcolatore, che quella volta le calcolatrici non c'erano ancora, e mise su la sua prima bluebox. Un aggeggio che attaccato al telefono permetteva di usarlo in barba a tutti.
Iniziava l'era dell'esplorazione sistematica della rete telefonica nazionale.
John se ne andò virtualmente - anche se questa parola ancora non era stata inventata - in giro per tutto gli States e anche oltre. Scoprì numeri per collegarsi a operatori dall'altro lato del continente, numeri riservati e un mucchio di cose segrete. Naturalmente lo spirito hacker era nel sangue: con le bluebox si potevano scroccare le chiamate, ma John e i suoi accoliti non scroccavano giusto per fregare il sistema con chiamate gratuite agli amici sull'altra costa. Usavano il marchingegno per esplorare, per conoscere e anche per migliorare: infatti quando trovavano una tratta telefonica bloccata o in qualche modo malfunzionante si mettevano in contatto con gli operatori di Ma Bell e comunicavano il guasto. Gli

di LOS ANGELES

addetti credevano che fossero colleghi che chiamavano da qualche posto sperduto. In realtà i nostri fecero così una delle più vaste operazioni di ingegneria sociale dell'epoca: dopo qualche tempo conoscevano per nome un sacco di dipendenti Bell.

Come War Games

A un certo punto degli anni 70 qualcuno incominciò a costruire i primi computer. Un certo Woz e un certo Steve, insieme in un garage, si dilettarono in una strana cosa che dotarono di tastiera e schermo video e che chiamarono Apple: una rivoluzione, in un'epoca in cui i computer sputavano dati solo su lucine colorate o al massimo su carta. Altri hacker progettarono altre macchine, come l'Altair, e anche il nostro John se ne procurò uno e progettò un nuovo modello di bluebox da infilare dentro al suo computer, in modo che questo potesse automaticamente chiamare una serie di numeri telefonici. Quando rispondeva un computer invece che un cristiano, zac!, ne prendeva nota. Tutto ciò ci ricorda il vecchio film War Games? Esatto, abbiamo capito da dove lo sceneggiatore ha tratto spunto.

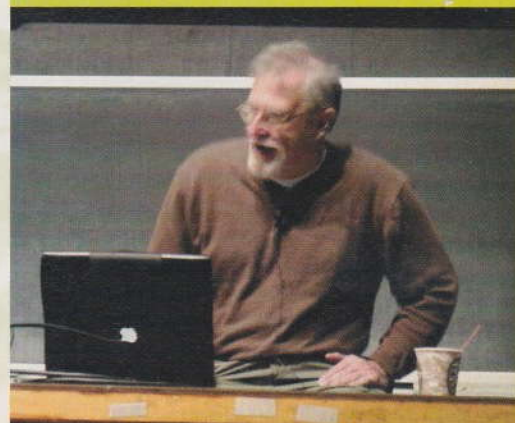
◄ *La mitica scatola con dentro il fischietto.*

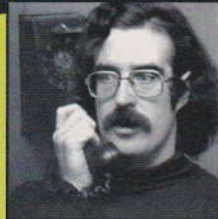
Olympus, please!

Tra tanti hack ed esperimenti vari c'era anche il tempo per divertirsi.
Una volta John, che era in compagnia di un paio di amici, aveva beccato un numero ultrariservato che collegava la CIA alla casa Bianca.
Trafficando coi toni della bluebox si era messo in ascolto automatico: tutte le chiamate che passavano su quella linea venivano trasmesse dall'altoparlante del suo laboratorio.
Un giorno sentirono addirittura un tizio della CIA che parlava col presidente Nixon in persona! Certo un Presidente degli Stati Uniti non viene a rispondere al telefono per ogni cavolata; ci vuole un buon motivo, e soprattutto la parola d'ordine: Olympus. Avevano la password per parlare col numero uno!
Manco a dirlo uno di loro si mise ad armeggiare con l'impianto e il telefono della Casa Bianca squillò, l'operatore rispose e: "Olympus, please!" - "Un attimo, per favore"... dopo un po' arriva Nixon alla cornetta: "Che succede?"
"Signor Presidente, è in atto una crisi qui a Los Angeles" - "Che tipo di crisi?" - "Siamo senza carta igienica, Signor Presidente!" Click.

Riccardo Ghiglianovich

Curriculum Vitae

John Draper aka Cap'n Crunch è stato arrestato un paio di volte per aver esplorato la rete telefonica degli Stati Uniti. Ha lavorato per la Apple, scrivendo il primo word processor per l'Apple II, poi comperato dalla IBM e portato dentro il primo PC IBM. Attualmente lavora in una società per la sicurezza informatica, e sta lavorando al CrunchBox, un Intrusion Prevention System basato su OpenBSD.

▲ *John Draper ricevette da un certo Danny un numero telefonico strano*

JohnD '70

◄ *All'epoca, John era così. Sempre attaccato al telefono.*

JohnD '04

► *Oggi, invece, pure: sempre attaccato al telefono.*

HACKING DELL'ALBERO DI NATALE

Facciamo del nostro albero di Natale un'esperienza straordinaria: ricco di luci e di colori e completamente programmabile...

Ci siamo mai chiesti come fare a collegare il nostro pc all'albero di Natale, per ottenere fantasmagorici effetti degni della nostra fama? La risposta è tutta contenuta in un po' di software libero e gratuito e nella porta parallela del nostro pc.
Con un po' di componenti esterni, pochi ed economici, possiamo pilotare a piacimento dei relè, senza scrivere una riga di codice. Quindi un progetto alla portata di tutti, ma se proprio non sappiamo o non vogliamo saldare qualche componente, è facile trovare un amico che in meno di mezza giornata sarà in grado di costruirci la basetta necessaria.

Il software

Per pilotare il tutto serve del software che riesca a dare corrente a ciascun piedino degli 8 che corrispondono ai dati in uscita dalla porta parallela. Naturalmente solamente quando lo vogliamo noi e sul piedino che decidiamo noi. Il software per le versioni di Windows più recenti lo possiamo scaricare gratuitamente all'indirizzo: www.kemo-electronic.com/download/RelaisTimer11.exe. La programmazione delle accensioni e degli spegnimenti di ciascun piedino la si fa visivamente con un clic

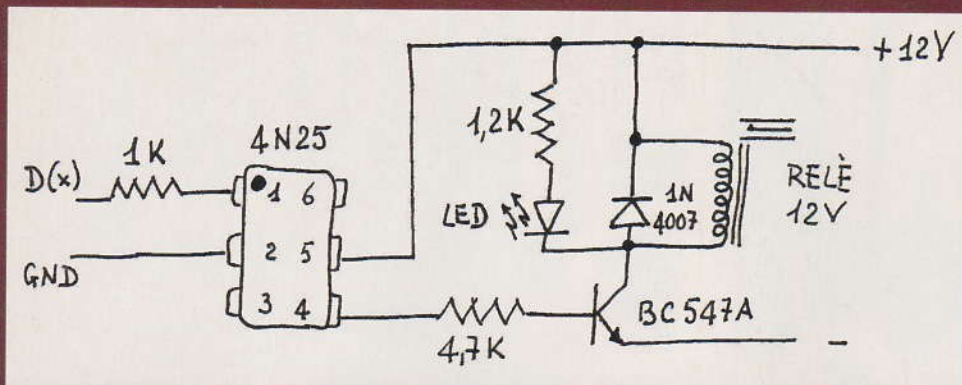
sui led simulati, nella colonna di destra. Con il pulsante Add si aggiunge ciascuna linea alla sequenza di programmazione, che appare a sinistra. La lista è ordinata sulla base dei tempi impostati. Quindi i tempi che si impostano sono il momento esatto in cui quella linea di predisposizione dei piedini viene eseguita. Questo significa che se si vuole, per esempio, fare in modo che tutti i relè si accendano per 2 secondi, poi si spengano per 2 secondi e così via, dovremo impostare questa sequenza:

La sequenza può essere resa ciclica spuntando la casella Loop, in basso, e se vogliamo può partire precisamente nel giorno e all'ora che impostiamo nella finestra Advanced Mode, che compare con un clic sul pulsante Edit.
Teniamo anche presente che i led simulati hanno tre stati: spenti, accesi e con una freccetta verso il basso. Questa significa solamente che viene mantenuto lo stato precedente, qualunque esso sia.
Verifica via software
Per sapere se la sequenza funziona o se vogliamo simulare il funzionamento dei relè senza avere ancora costruito la basetta, dobbiamo procurarci un software capace di leggere i registri della porta parallela. Si chiama lpt parallel port monitor e lo si scarica all'indirizzo http://neil.fraser.name/software/lpt/lpt.exe. Se lo facciamo funzionare mentre eseguiamo una sequenza di Relais Timer, vediamo indicate le linee che vanno a on. L'unica attenzione che dovremo avere è provare a selezionare LPT1 o LPT2 o LPT3 senza preoccuparci se non corrispondono a quanto abbiamo configurato in Kemo-relais timer nel menu Optino > Configuration. Capita che i due software attribuiscano a indirizzi uguali porte differenti, ma poco ci importa.

Costruzione dell'interfaccia

Il circuito si realizza tutto in mezza giornata o meno, con un po' di pazienza e un po' di pratica con il saldatore. Si tratta di seguire lo schema per ogni linea che vogliamo usare, quindi al massimo si può replicare otto volte, per pilo-

+ 00.000	X X X X X X X X	Inizio
+ 02.000	0 0 0 0 0 0 0 0	Accensione dopo 2 secondi
+ 04.000	X X X X X X X X	Spegnimento dopo 2 secondi

Con qualche software libero e un po' di fantasia possiamo relizzare l'albero di Natale che abbiamo sempre desiderato.

Questo è lo schema per controllare un relè. Ne possiamo costruire fino a 8, tanti quanti sono i bit che riusciamo a pilotare dalla porta parallela. L'optoisolatore 4N25 al suo interno contiene un led e un fototransistor (sensibile alla luce). Così il pc rimane isolato e protetto.

tare otto dispositivi differenti e autonomi. Funziona con certezza al primo colpo.
Lo schema prevede che il segnale prelevato dalla porta parallela del computer sia inviato a un optoisolatore. Dentro questo piccolo componente la corrente è trasformata in luce accendendo un led interno al chip, il quale illumina un transistor sensibile, ottenendo così di avere un dispositivo che, alimentato, riconverte la luce in corrente elettrica. L'effetto è quello che tra le nostre lampadine di natale e il computer non c'è assolutamente nulla in comune: né la massa, né l'alimentazione. I due circuiti sono completamente separati da un raggio di luce e quindi è impossibile rovinare la porta del computer anche se dovessimo sbagliare qualche cosa sul circuito dei relè.
L'uscita dell'optoisolatore 4N25 pilota un transistor BC547 (per nulla critico, lo troviamo anche in tutti i vecchi televisori), capace di attivare il relè. In parallelo alla bobina del relè abbiamo messo anche un led, che ne indica l'attivazione e quindi il segnale a 1 in uscita dalla porta del pc.Il diodo 1N4007 in parallelo (ma con la polarità invertita) alla bobina del relé serve per salvare il transistor dalle extracorrenti che si generano quando la bobina del relè si disattiva.
All'uscita del relè possiamo collegare tutto quello che vogliamo, senza superarne le possibilità. Un relè miniatura pilota in genere poco più di 1 ampere. Uno come quelli che abbiamo usato noi fino a 10 ampere, a 230 V. Più che sufficiente per attaccare qualunque carico di lampadine.
Il relè ha tre piedini in uscita: con uno possiamo attivare un dispositivo quando il bit della porta parallela è disattivo a 0, con l'altro viceversa, quando è attivo a 1.
A noi sfruttare le infinite possibilità.
Buon divertimento e buon Natale!

StandardBus
standardbus@softhome.net

Una sequenza di accensioni sulla linea uno, appena costruita, per verificare il funzionamento dello schema. Perfetto, funziona al primo colpo. Ora replicheremo per otto.

L' ELENCO DEI COMPONENTI NECESSARI

- » 1 resistenza 1 Kohm, 1/4 W
- » 1 resistenza 1,2 Kohm, 1/4W
- » 1 resistenza 4,7 Kohm, 1/4 W
- » diodo 1N4007 (o similare)
- » transistor NPN BC547A (o equivalente)
- » optoisolatore 4N25
- » relè 12V, 55mA (230V, 5A sui contatti)
- » alimentatore 12 V, 1A

connettore parallelo 25 pin maschio
piattina 10 conduttori e connettore da circuito stampato
eventuali morsettiere per il collegamento dei relè e per l'alimentazione a 12V

FACCIAMO ATTENZIONE

La porta parallela è spesso integrata nella piastra madre del computer. Se qualcosa va storto il rischio è quello di dover sostituire o riparare l'intera scheda madre. Ecco perché usiamo gli optoisolatori: qualunque cosa succeda alle nostre lampadine natalizie, tutta la parte "di potenza" del circuito è isolata otticamente dal computer e quindi non è possibile che avvengano dei ritorni di corrente che potrebbero danneggiare il pc. Ovviamente solamente se abbiamo fatto le cose bene, seguendo lo schema. L'autore e l'editore, naturalmente, non si prendono nessuna responsabilità. Fate tutto a vostro rischio e pericolo.

HAI MAI PROVATO FreeBSD?

Il software libero è un universo di cui Linux è una galassia importante. Ma le galassie sono tante e una delle più interessanti è questa

Molti non sanno neanche che esistono alternative a Windows. Qualcuno lo sa e pensa che esistano solo Macintosh e Linux. Notizia per tutti: i sistemi operativi sono tanti. Uno dei più interessanti, potente, sicuro, libero, gratuito, è FreeBSD.

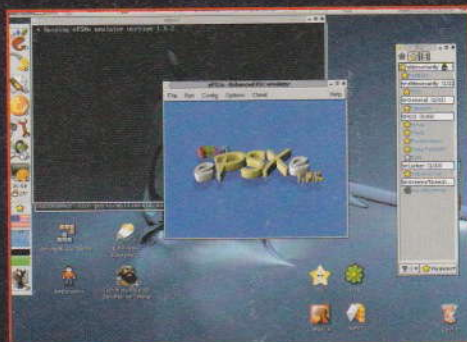
Anche lui è un derivato di Unix, come Linux, ma è nato ben prima, da una costola del sistema BSD creato in California presso l'Università di Berkeley, vicino a San Francisco.

Funziona dappertutto

FreeBSD funziona praticamente su qualsiasi processore esistente, Pentium, Athlon, AMD, Opteron, EM467, ma anche il PowerPC dei Macintosh e Alpha, Itanium, PC-98, UltraSPARC, MIPS e qualcun altro ancora. Non c'è computer prodotto negli ultimi dieci anni che non possa montare FreeBSD.

Come si usa

Essendo un sistema di tipo Unix, FreeBSD può essere guidato mediante un'interfaccia grafica oppure via comandi testo digitati dentro una shell (praticamente un editor di testo partico-

lare). Chi ha sperimentato Mac OS X o Linux sa perfettamente di che cosa parliamo. Anche su Windows è possibile fare molto con il Prompt di comandi MS-DOS, che è un ambiente simile.

Che cosa si può fare? Tutto. Tutti i più famosi programmi open source sono disponibili su FreeBSD. OpenOffice può leggere tutti i documenti creati con Office di Microsoft. Si può navigare nel Web con Mozilla, leggere le mail, qualsiasi cosa, con l'interfaccia grafica che desideriamo, sia Gnome oppure un'altra.

Qualche esempio di comando

Supponendo di usare la shell e non l'interfaccia grafica, ecco qualche esempio dei comandi da dare. Seguiamo la tradizione Unix e indichiamo con % quello che viene digitato da un utente normale: root sarebbe #.

%adduser
aggiunge un nuovo utente

% exit
esegue il logout

% id
spiega chi siamo dentro il sistema

% pwd
mostra la directory di lavoro corrente

% ls
elenca i file nella directory corrente

% cat
mostra il contenuto di un file sullo schermo

% apropos
consulta il database whatis e dice quali comandi svolgono una certa funzione

% rm
cancella file

Chi conosce Linux o Mac OS X si accorgerà che le differenze sono minime o nulle.

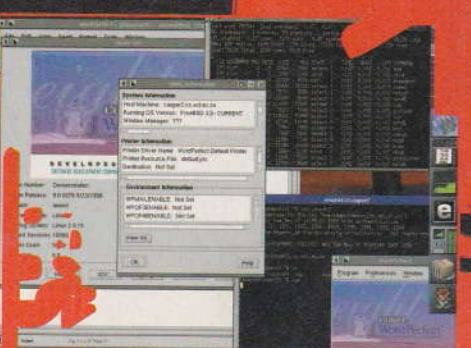
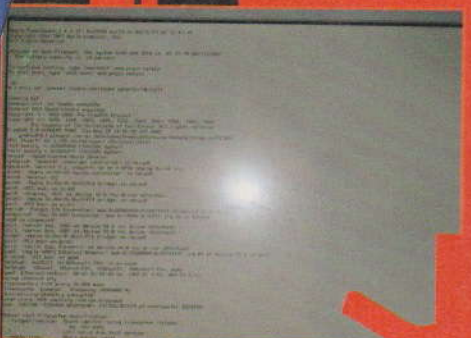
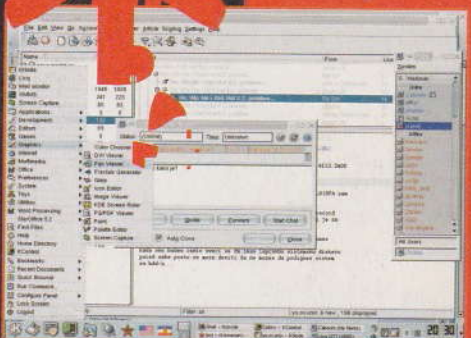
Ma allora, dirà qualcuno, perché non usare Linux o Mac OS X? Perché la diversità fa bene all'evoluzione, perché FreeBSD monta un motore interno (il kernel) piuttosto differente da Linux. Questo lo rende, per esempio, mediamente più sicuro. Inoltre sapere usare più sistemi operativi è come sapere più lingue: tiene allenato il cervello e per hacker come noi è essenziale!

Torneremo presto a parlare di FreeBSD entrando più nello specifico. Chi è interessato lo faccia sapere!

Beth
i5b3773r@mac.com

L'ESSENZIALE SU FREEBSD

Il sito di riferimento di FreeBSD è ovviamente http://www.freebsd.org (consultabile anche in italiano!), dove si trovano anche l'elenco delle piattaforme supportate e un sacco di link alle risorse più varie, tra cui i programmi utilizzabili e le FAQ, oltre a un elenco di programmi già pronti (http://www.freebsd.org/applications.html) e porting da altre piattaforme (http://www.freebsd.org/ports/index.html). All'indirizzo http://www.freebsd.org/projects/newbies.html c'è anche un link apposta per i nuovi arrivati che non sanno niente di Unix o di FreeBSD.

Per recuperarlo si parte da http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/mirrors.html. Chi ha una buona connessione a Internet può installarlo direttamente via Rete, partendo da un paio di vecchi floppy disk.

VULNERABILITA' DI UN CHIOSCO

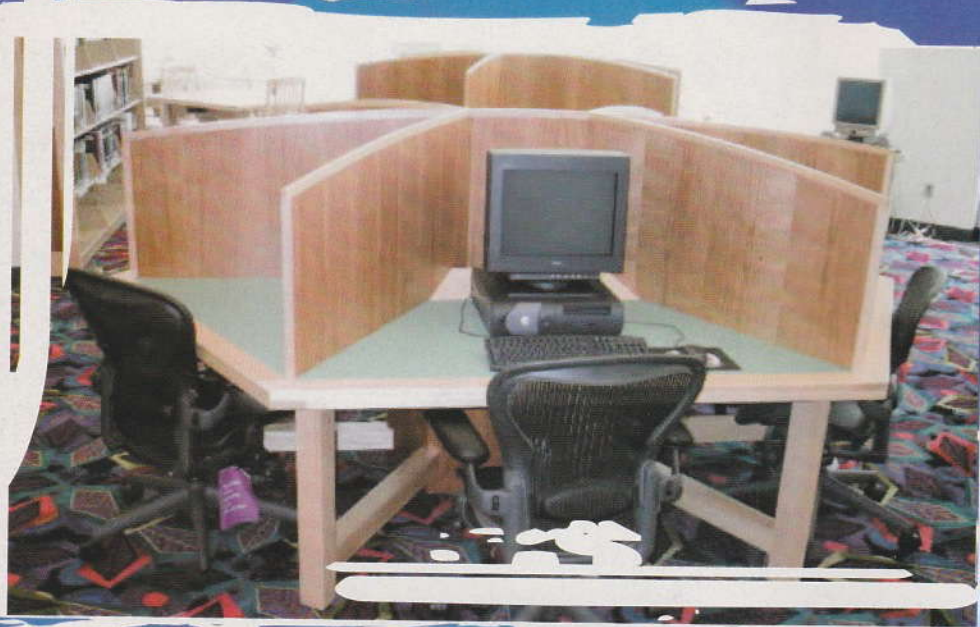
Da qualche anno sono presenti in molti luoghi, spesso pubblici, dei terminali detti "chioschi", tramite i quali è possibile accedere a diversi servizi. Ne sono un esempio quelli installati presso le biblioteche, utili per accedere ai così detti "cataloghi online" e quindi rintracciare libri e materiale multimediale.
I suddetti terminali permettono l'accesso a Internet in modo molto controllato. Il gestore del chiosco ha la facoltà di permettere l'accesso solamente a pochi e ben mirati siti, generalmente inerenti gli argomenti relativi all'utilizzo del chiosco oppure a servizi che si ritengono d'interesse per l'utente. Nel caso delle biblioteche, se rimaniamo nell'esempio fatto, è facile trovare la possibilità di accesso ai soli siti di enti pubblici in qualche modo legati al luogo dove il chiosco è installato. Per esempio, è possibile accedere al sito istituzionale della regione, del comune, o a qualche indirizzo di ministeri e associazioni culturali, e così via. La navigazione libera è invece quasi sempre impedita, anche perché il gestore del chiosco, come di ogni altro punto di accesso Internet aperto al pubblico, avrebbe degli obblighi di legge da rispettare, che sarebbero l'esatta identificazione dell'utente che sta utilizzando il tutto, per evitare o scoraggiare usi illeciti (spamming, scaricamento di risorse illegali, eccetera).

Un exploit imprevisto

Una grande quantità di sistemi autonomi installati nei luoghi pubblici è basata su SiteKiosk, un programma che troviamo all'indirizzo www.sitekiosk.com, distribuito anche in versione shareware; versione sulla quale possiamo fare le nostre prove. In pratica può accadere che il programma in questione sia configurato male e senza tutte le attenzioni dovute. In particolare, l'errata impostazione del sistema utilizzato per blindare i ter-

PERFINO IN RETE

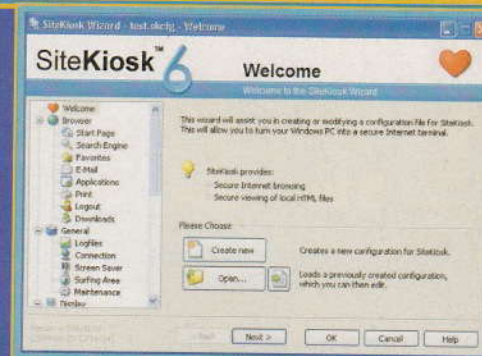
I terminali-chioschi, in genere, hanno una caratteristica. Non sono veri e propri pc stand-alone, ma sono configurati per accedere in rete tutti allo stesso hard-disk. Per cui, in realtà, la nostra configurazione spesso e volentieri è stata installata sull'hard disk del server centrale remoto e una volta creata potremmo usarla sempre, perché la ritroveremmo su qualsiasi terminale di qualunque luogo collegato allo stesso server, ovunque esso si trovi.

I chioschi informativi pubblici sono sistemi blindati che non permettono di accedere a Internet liberamente. Ma siamo sicuri che siano stati configurati correttamente? Perché in teoria sarebbe possibile che...

minali verso l'esterno (=Internet!) e del sistema in generale, ci permetterebbe di creare nuove configurazioni senza alcuna restrizione e quindi far partire un'altra finestra con la nostra configurazione, che ovviamente comprenderebbe i permessi di navigare indisturbati.

Una seduta alternativa

La questione, dopo un po' di prove fatte sul software e immaginandoci davanti a un terminale, potrebbe avvenire esattamente come la descriviamo. Se nella realtà dovessimo accorgerci che effettivamente è possibile agire in questo modo, dovremo sentirci in obbligo di avvertire il gestore del chiosco, perché ovviamente possa prendere i provvedimenti adeguati, ovvero possa riconfigurare il sistema così da metterlo in sicurezza.

Assicuriamoci di essere alla pagina iniziale con un un clic su "start", presente sulla barra in alto al centro. Da qui selezioniamo una delle icone presenti. Generalmente, se per esempio fossimo in una biblioteca, una sarebbe probabilmente dedicata ai libri e l'altra alla sezione multimediale. Stiamo quindi entrando nel sistema.

Ora selezioniamo un banner relativo a un sito la cui visita è permessa. Supponiamo sia quello della regione di competenza: in genere c'è sempre, perché questi sistemi sono spesso sponsorizzati (=finanziati) da organi regionali. All'interno del sito che abbiamo raggiunto cerchiamo quindi qualsiasi documento scaricabile, per esempio un probabile documento pdf. Per farlo possiamo usare la casellina di ricerca, in genere sempre presente sui siti in questione.

Nel campo "cerca" è sufficiente scrivere "pdf" o ".pdf". Selezioniamo quindi un risultato a caso tra tutti quelli ottenuti.

Lo scopo di tutto ciò sarebbe quello di accedere all'hard disk del terminale.

Bene! Ci verrà chiesto se vogliamo aprire il documento oppure salvarlo!

Un clic su salva, poi un clic su "c:\" e così ci spostiamo in Programmi e poi nella cartella SiteKiosk. Assicuriamoci che nel campo "salva come" sia specificato "tutti i file". Appare anche il file Configure.exe. Selezioniamolo con un solo clic e poi col tasto destro scegliamo "apri". Ovviamente non avremo i permessi per modificare le configurazioni esistenti, ma nulla ci vieta di creare una configurazione ex-novo su misura ai nostri scopi!

Non ci resta altro che configurare la nostra finestrella per il web. Ricordiamoci tra le altre cose di far visualizzare la barra per l'immissione degli url e il tasto close per chiudere la finestra, dopodiché diamo un nome a questa nuova configurazione e salviamola.

Per aprire un'altra finestra lanciamo Sitekiosk (in C:\Programmi\SiteKiosk\ apriamo il file sitekiosk.exe, nello stesso modo in cui abbiamo eseguito configure.exe). Se appare qualche pop-up di warning è sufficiente un clic su ok, fino a che non spunta la schermata che ci chiederà quale file di configurazione utilizzare. Selezioniamo il nostro file appena creato, e andiamo avanti con la procedura...

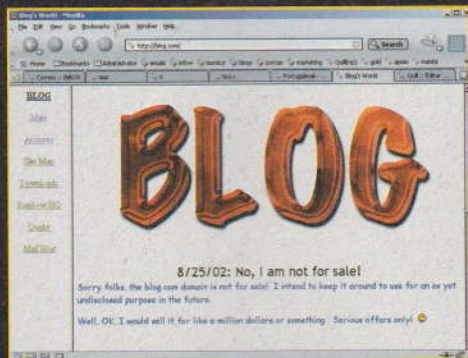
Così facendo potremmo navigare su Internet anche con il terminale di un chiosco, basato su SiteKiosk, male configurato.

Francesco "EthMan" S.

UN BLOG DAVVERO PER

ACCESSIBILITÀ: la scienza che si occupa di rendere i siti Web accessibili a chiunque. Questi consigli li dà solo Hacker Journal

Abbiamo visto nel numero 58 di HJ come sia sempre opportuno specificare il DOCTYPE corretto nei documenti HTML che scriviamo. Vale per i blog e anche per i siti normali (dopotutto un blog è solo un sito un po' particolare). In questo numero vediamo innanzitutto l'importanza della lingua. Anche se può sembrare strano, specificare che lingua parla il nostro sito è fondamentale per il suo successo. Prima di tutto, chi naviga con sistemi di sintesi vocale (per esempio i non vedenti) ha software che può adattarsi alla lingua parlata dal sito.

Anche se i non vedenti non ci interessassero, comunque, dovremmo fare attenzione. Secondo Google Zeitgeist (http://www.google.it/press/zeitgeist.html, da vedere!), metà degli utenti di Internet

ricercano su Google parole in una lingua diversa dall'inglese. Di questi una percentuale significativa è in italiano e non vogliamo perderla, giusto? Solo che se il nostro programma di authoring HTML inserisce una lingua sbagliata senza che ce ne accorgiamo, o non ne inseriamo nessuna, rischiamo che Google non trovi il nostro sito! Molti configurano addirittura le Preferenze di Google (http://www.google.it/preferences) in modo da cercare solo nella propria lingua o in lingue specifiche. Google dovrebbe trovarci ugualmente perché ha ottimi algoritmi, ma perché rendergli il lavoro difficile, con tutte le pagine che si fanno trovare facile?

Impostare la lingua

Serve il giusto identificatore di nazione. Se il codice per l'inglese è en, quello per il francese è fr e quello per il tedesco è de, quale potrà essere quello per l'italiano? it, naturalmente. L'elenco completo di tutti i codici identificativi del mondo, per gli interessati, si trova a http://www.oasis-open.org/cover/iso639a.html. I codici si possono

scrivere in maiuscolo o in minuscolo e funzionano sempre. Ma dove si scrivono? Dentro il tag <html>. Come, esattamente, dipende dal DOCTYPE. Vediamo qualche esempio.

- **HTML o sua variante**

Cambiamo il tag

```
<html> in <html lang="it">
```

(cambiando la lingua se serve qualcosa di diverso dall'italiano)

- **XHTML 1.0 o sua variante**

Cambiamo il tag

```
<html> in <html xmlns="http://www.w3.org/1999/xhtml" lang="it" xml:lang="it">
```

- **XHTML 1.1 o sua variante**

Cambiamo il tag

```
<html> in <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="it">
```

Come succede con DOCTYPE, bisognerebbe identificare la lingua su tutte le pagine del sito.
Se su una pagina compare più di una lingua, non c'è problema. Per esempio, se abbiamo il blog in italiano ma ci sono citazioni in inglese, possiamo organizzarci come segue. L'esempio vale per pagine con DOCTYPE tipo HTML.

```
<html lang="it">
...
<blockquote lang="en">
...
</blockquote>
```

Per sapere tutto, ma proprio assolutamente tutto, su come funziona l'attributo lang, bisogna studiare con attenzione la pagina http://www.w3.org/TR/REC-html40/struct/dirlang.html#h-8.1.

Dare titoli significativi alle pagine

Ogni pagina Web che creiamo dovrebbe avere un titolo significativo. Nel caso di un blog, la pagina home potrebbe semplicemente avere il nome del blog, ma dovrebbe almeno avere il nome del blog! Ci sono in giro lameroni che lasciano le pagine senza titolo, oppure riempiono i titoli di sciocchezze. Queste, al massimo, dentro la pagina, ma non nel titolo. Le pagine di archivio, se sono organizzate per data, dovrebbero compren-

FARSI UN BLOG

Programmi per farsi un blog come si deve

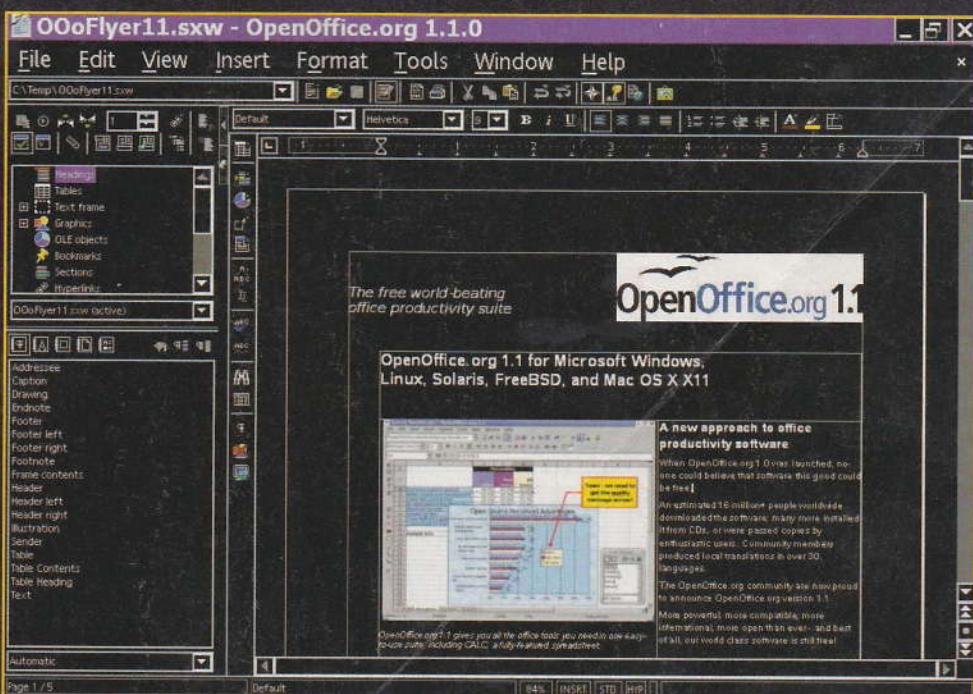
MOVABLE TYPE
http://movabletype.org

GREYMATTER
http://www.noahgrey.com/greysoft/

BLOGGER
http://www.blogger.com

SPLINDER
http://www.splinder.com

USERLAND
http://www.userland.com

MANILA
http://www.userland.com

Un'interfaccia particolare per chi fatica a muovere il mouse con destrezza.

dere il nome del blog, seguito dalla data o dall'intervallo delle date, per esempio Blogico/19 dicembre 2004 oppure Bloglob/dicembre 2004. Altro trucco utile per ordinare in fretta le pagine è numerarle secondo anno (a quattro cifre), mese (due cifre) e giorno (due cifre). Per esempio, 4 dicembre 2004 = 20041204. Anche in ordine alfabetico i file saranno in ordine di data.

Se ci sono categorie, sarebbe meglio includerle nel titolo della pagine assieme al nome del blog: Mioblog/politica (se si parla di politica). A essere bravi, ogni singola pagina, dedicata a un singolo argomento, dovrebbe contenere nel titolo il nome del blog e l'argomento in questione: Bloggheria: Ecco perché è meglio Perl di Python.
Come per la lingua, i programmi di lettura per non vedenti fanno caso al titolo delle pagine e per loro è quindi un bel vantaggio. Ma, se anche fossimo cattivi, comunque ci converrebbe, perché Google privilegia le pagine con un titolo. I motori di ricerca, in generale, ignorano quello che c'è in un titolo dopo i primi 50 caratteri.

P. Greco
p.greco@hackerjournal.it

PER CHI NON VEDE

Per navigare un sito anche se si è non vedenti.

Programmi come JAWS permettono di condurre una vita normale su internet anche a persone con problemi di vista. Se i siti sono male organizzati, però, anche il programma giusto serve a poco. JAWS è per Windows ma esistono cose simili per tutti i sistemi operativi. http://www.freedomscientific.com/fs_products/software_jaws.asp.

I lameroni con loro non la passano liscia

Buffer Overflow

Un buffer overflow avviene quando un processo tenta di memorizzare più dati di quelli che ci stanno, in una zona di memoria destinata ad accoglierli temporaneamente (buffer). Le informazioni di troppo traboccano (overflow) in zone di memoria adiacenti e gli effetti possono essere devastanti, sia per i dati presenti in memoria, sia perché i dati in eccesso possono essere dei veri e propri programmi che scatenano operazioni specifiche.

ESEMPIO

Un programma ben congegnato e introdotto in un computer tramite una debolezza di sistema che consenta il buffer overflow, potrebbe alterare i file, distruggere dati, acquisire password. Dipende dal zona di memoria in cui riesce a introdursi e dai privilegi che riesce a conquistarsi.
Un semplice buffer overflow si potrebbe verificare anche supponendo, per esempio, di partire da un form su web programmato per accettare dieci caratteri (tramite un parametro maxlenght=10). Quando il form viene inviato, il server si aspetta in arrivo una stringa di caratteri che potrebbe essere qualcosa come:

```
http://www.underflow.com/pubs/test.html?username=a
lessandro
```

Se però gli venisse inviata una stringa come:

```
http://www.underflow.com/pubs/test.html?username=a
lessandrozzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz
zzzzzzzzzzzzzzzzzz
```

e se il sistema non fosse protetto dai buffer overflow, il tutto potrebbe cadere in crash o, peggio ancora, lasciare passare l'utente in quanto situazione non prevista dal sistema di autenticazione.

Requisiti

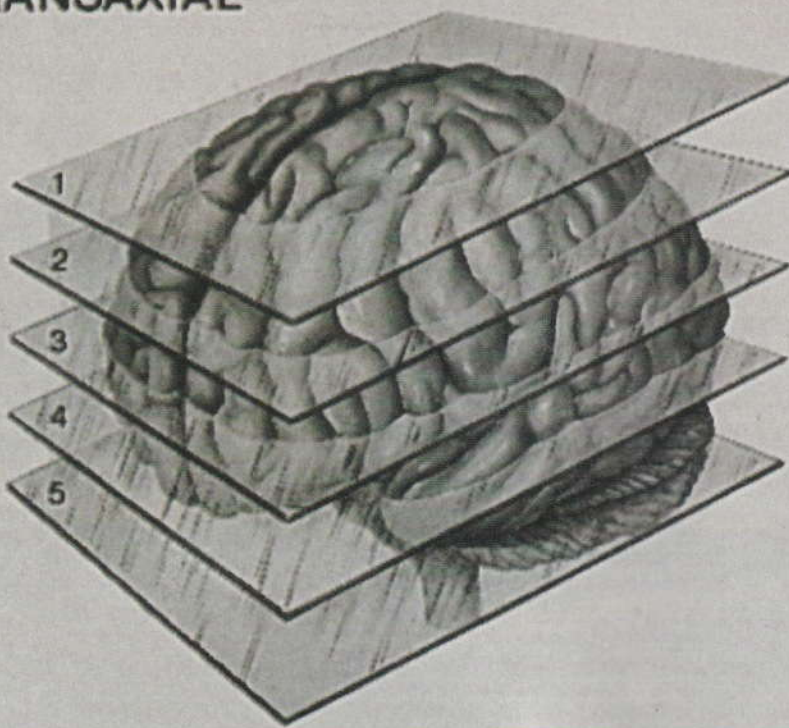
La conoscenza del C è spesso utile per studiare i buffer overflow. I programmi scritti in C sono infatti quelli generalmente più soggetti a presentare falle di questo tipo, perché il C richiede al programmatore di controllare la lunghezza dei buffer di memoria. I programmi scritti in linguaggi come VisualBasic o Java sono generalmente meno soggetti a questo tipo di attacco.

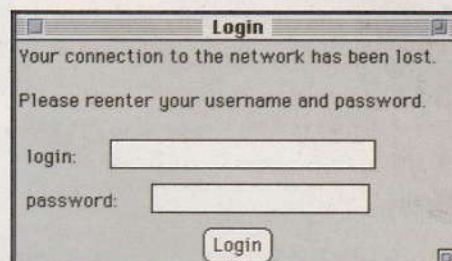
Security

Molto spesso gli attacchi di buffer overflow vanno a buon fine perché il sistema attaccato fa funzionare i suoi processi di rete direttamente nella root o comunque a livello di amministratore di sistema. È quindi più facile per chi attacca fare girare programmi devastanti da un livello che ha privilegi così alti.
La prima precauzione è far funzionare i programmi che servono a livelli più bassi, cioè senza i privilegi di amministratore di sistema.

LINK:
Un esempio di buffer overflow verificatosi su sistemi di un paio d'anni fa: http://project.honeynet.org/scans/scan25/sol/NCSU/main.html#b6
Un recente buffer overflow scoperto possibile tramite le immagini .png: http://scary.beasts.org/security/CESA-2004-001.txt

ENCICLOPEDIA dell'Hacking!

Ingegneria sociale

L'ingegneria sociale è una forma di hacking che si interessa più alla mentalità dell'utilizzatore di un computer piuttosto che al computer stesso.
Lo scopo è quello di acquisire quante più informazioni possibili su un utilizzatore di sistemi informatici per capirne i punti di forza e di debolezza nell'uso dei sistemi stessi.

Login
Your connection to the network has been lost.
Please reenter your username and password.
login:
password:
Login

ESEMPIO

L'ingegneria sociale prende spunto dalle situazioni più diverse. È ingegneria sociale la classica telefonata che ricevono i centralini delle aziende con i tentativi più originali di farsi dire il nome di un impiegato. È ingegneria sociale il tentativo, legalmente perseguibile, di chi cerca di carpirci il numero della carta di credito spacciandosi per l'impiegato della banca. È ingegneria sociale lo sguardo sfuggente di chi ci sta alle spalle in pizzeria e riesce a memorizzare (ci riescono, ci riescono...) il numero del pin che digitiamo sul bancomat.
Ingegneria sociale è quindi una questione spesso di psicologia, a volte di destrezza, quasi sempre di furbizia.
Strumenti dell'ingegneria sociale sono anche, per esempio, le ricerche sulle pagine bianche o gialle, o sulle mappe stradali. Le prime ci diranno molte cose a partire da un semplice telefono, o da un nome, o da una denominazione di una società. Conosciuto l'indirizzo, potremo spesso individuare lo stato sociale e quindi

approssimativamente dedurre la fascia di reddito a partire dalla zona in cui abita il soggetto. E così via, senza limiti alla fantasia, ma facendo attenzione a non infrangere le leggi sulla privacy.

Requisiti

Per essere dei buoni ingegneri sociali bisogna studiare il comportamento delle persone e capire come si comportano, in maggioranza, a fronte di situazioni impreviste o velate sensazioni di disagio. "Non me lo può dire lei, senza dover per forza coinvolgere il suo capo?..." è per esempio una frase che denota profonda conoscenza delle debolezze aziendali. Poi è necessario conoscere gli strumenti che si possono avere a disposizione per acquisire le informazioni più diverse.

Security

L'ingegneria sociale si combatte con la sicurezza di ciò che si è e che si sta facendo, con il ragionamento e con la scrupolosa metodicità nel seguire procedure collaudate. Semmai, chi va in crisi potrà essere una procedura, ma non noi. L'ingegneria sociale, in fondo, si combatte con gli stessi mezzi dell'ingegneria sociale...

LE MAPPE STRADALI:
www.viamichelin.it

PAGINE BIANCHE E GIALLE:
www.paginebianche.it
www.paginegialle.it

MAPPE AEREE DELL'ITALIA E DEL MONDO
www.atlanteitaliano.it
www.keyhole.com

Da staccare e conservare nel tuo raccoglitore

PALLA DI CRISTALLO: LE RISPOSTE

OVVERO: QUANDO FINIRÀ IL TEMPO DI UNIX. IN TEORIA, NATURALMENTE

Le domande di HJ 61 riguardavano da una parte gli stereogrammi, dall'altra gli orologi interni dei sistemi operativi, Unix in testa. L'immagine-enigma era questa:

Le domande

PER TUTTI: qual è la data? Il 2038! Come si chiama una immagine come quella sopra? Stereogramma!
PER ESPERTI: che cosa succederà a Unix in quella data? Si esaurirà l'orologio di sistema. Ci sono siti e programmi per fare stereogrammi?
PER GENI: quali sono le date corrispondenti per Windows e Macintosh? Sei capace di produrre uno stereogramma? Con dentro la data opposta a quella del 2038?
PER SUPER HACKER: sai produrre uno stereogramma con un programma? Sai produrre un programma per decodificare stereogrammi?

Le risposte

Primo arrivato, ed esperto: MatteoGeniaccio - dedicato ad Arianna! Matteo scrive: Nel 19 gennaio 2038 alle ore 3, 14 minuti e 7 secondi i sistemi Unix avranno un problema simile al millennium bug (http://www.autorita.energia.it/docs/pareri/millennium.htm). Una guida si trova su http://www.ffranceschi.com/midima/stetuit1.html, mentre alcuni programmi sono su http://www.tuttogratis.it/software_gratis/software_gratis_creazione_stereogrammi.html. Bravo Matteo!
PER TUTTI: nibbio scrive: il 19 gennaio del 2038, alle 03:14:07 di T.U. (tempo universale, le 4 in Italia), i contatori del tempo dei sistemi Unix a 32 bit dovrebbero smettere di funzionare, perché saranno passati 2.147.483.647 secondi dalla nascita di Unix (1 gennaio 1970). 2.147.483.647 è il massimo intero positivo contenuto in un signed integer (4 byte, 32 bit), pari a 2^32/2-1. Naturalmente per quell'epoca ci saranno, si spera, in funzione sistemi operativi a 64, 128, 256 bit... e chissà che altro... Poi: claudioalbatros e naqern.
PER ESPERTI: NastyBit aggiunge che l'inizio del tempo Unix si chiamava Tempo Zero (o epoch) e che alla scadenza gli orologi Unix attuali si riazzereranno, pensando che sia il primo gennaio 1970. Ma per il 2038 una nuova versione di Unix avrà certamente risolto il problema.
I vecchi Mac andranno in crisi nel 2040, i sistemi NT nel 2099. Siti per stereogrammi: programmi per farli a _ http://www.alc-wbc.com/products/bigle3d/index-en.html _ BIGLE3D oppure _ http://www.ixtlan.ru, e tutorial a http://www.ffranceschi. com/midima/stetuit1.html.
PER GENI: vagabondo ha mandato un trattato. Lo pubblichiamo in un prossimo numero! Poi _<=Hacker89=>_.
PER SUPER HACKER: Ezio Rizzo, che è stato sensazionale, scrivendo in QBasic 4.5

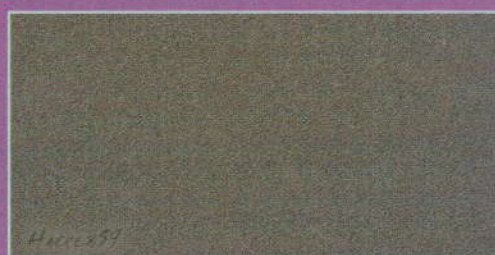
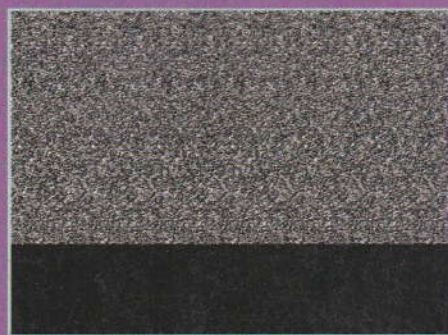
PERL FOR UNIX

Per vedere se un sistema Unix ha problemi con l'anno 2038 basta eseguire questo script Perl:

```
#!/usr/local/bin/perl

use POSIX;
$ENV{'TZ'} = "GMT";

for ($clock = 2147483641; $clock <
2147483651; $clock++) {
        print ctime($clock);
}

# Output corretto per Sistemi unix non
dipendenti:
#
# Tue Jan 19 03:14:06 2038
# Tue Jan 19 03:14:07 2038 <— PUNTO
DI ROTTURA
# Tue Jan 19 03:14:08 2038
```

<=Hacker89=> e il suo stereogramma!

Ezio Rizzo. Ha programmato tutto il necessario. Complimenti!